Informatiebeveiligingseisen aan Leveranciers van dataleveringen (Wibon)

Afdeling Cybersecurity dd. 23-07-2025

ProRail levert op basis van wettelijke verplichtingen (Wibon, INSPIRE, EC61) gegevens aan het Kadaster over bovengrondse en ondergrondse netten. Voor deze gegevensuitwisseling maakt ProRail momenteel gebruik van een applicatie van Geodan/Sogelink.

Van de serviceprovider wordt verwacht dat deze een stabiele, toekomstbestendige en juridisch conforme oplossing biedt, waarbij ook eisen op het gebied van informatiebeveiliging worden geborgd.

Deze eisen zijn als volgt:

* Alle rood gemarkeerde hoofdstukken zijn niet van toepassing verklaard.

A. AVG*

B. Awareness

a. De leverancier zorgt ervoor dat gedurende de uitvoering van het contract zijn medewerkers periodiek en aantoonbaar op het belang van informatiebeveiliging en hun rol daarin worden gewezen (security awareness).

C. Bedrijfscontinuïteit*

D. Certificeringen en normenkaders*

E. Contactpersoon

a. Zowel ProRail als de leverancier hebben een contactpersoon voor informatiebeveiligingsaspecten, vastgelegd in bijvoorbeeld de SLA. Deze contactpersonen zijn adviserend en ondersteunend aan het contract- en leveranciersmanagementproces. Afstemming vindt altijd plaats onder regie van de contractmanager.

F. Escrow*

G. Exit-strategie*

H. Gegevensuitwisseling

a. Digitale gegevensuitwisselingen vinden plaats conform een gestandaardiseerde en beveiligde manier.

I. Gegevensverwerking en -opslag

a. De leverancier maakt alleen gebruik van de verstrekte en gegenereerde gegevens voor het uitvoeren van de gecontracteerde werkzaamheden.

b. Indien informatie opgeslagen wordt binnen de infrastructuur van de leverancier, dient deze beveiligd te worden conform het beveiligingsniveau dat bij deze informatie is overeengekomen. Dit betekent dat persoonsgegevens per definitie minimaal als Vertrouwelijk geclassificeerd zijn. (Bij bijzondere persoonsgegevens : Geheim)

c. De websites, servers en databasesystemen met alle daarop opgeslagen informatie bevinden zich fysiek binnen de Europese Economische Ruimte (EER) en mogen alleen vanuit een locatie buiten de EER toegankelijk zijn en/of bewerkt worden vanaf een beveiligd werkstation

waarbij lokale opslag niet mogelijk is en een beveiligde verbinding en multi-factor authenticatie gebruikt wordt. De data mogen de EER niet verlaten.

J. Geheimhouding*

K. Incidenten

a. Bij constatering van een kwetsbaarheid, beveiligingsincident of datalek dient de leverancier onverwijld contact op te nemen met de Centrale Servicedesk van ProRail, bereikbaar op nummer 0882312600, en de betreffende contractmanager.

L. Monitoren en loganalyse

a) Activiteiten van gebruikers en beheerders dienen ten behoeve van audittrailing passend beveiligd vastgelegd te worden in logboeken. Deze registratie wordt op verzoek van ProRail door de leverancier op een door ProRail te definiëren wijze beschikbaar gesteld.

M. Onderaanneming en toeleveranciers

a. Alle voorwaarden en eisen op het gebied van informatiebeveiliging die gelden voor de leverancier zijn ook van toepassing op derden, die in opdracht van de leverancier diensten verrichten voor ProRail.

N. Periodiek overleg en rapportages*

O. Personeel

b. Extern personeel dient zich te houden aan de gedragsregels van ProRail.

P. Retour/vernietiging bedrijfsmiddelen en informatie

a. Op verzoek retourneert of vernietigt de leverancier, dit naar keuze van ProRail, onverwijld alle door ProRail ter hand gestelde documenten, boeken, bescheiden en andere zaken (waaronder begrepen gegevensdragers en back-ups). Dit geldt ook voor alle gegevens, inclusief persoonsgegevens, ook in cloudomgevingen.

Q. Auditrecht

a. ProRail kan op enig moment een audit, waaronder een penetratietest (laten) uitvoeren om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan. Dit gebeurt in overleg met de leverancier. Een audit is niet nodig als de leverancier door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd, dan wel aantoont dat een onafhankelijke audit heeft plaatsgevonden en de relevante resultaten deelt met ProRail.

R. Risicomanagement

a. De leverancier dient ProRail (op verzoek) te informeren over de getroffen beheersmaatregelen die relevant zijn binnen het kader van de dienstverlening.

S. Security en BCM by Design*

T. Security testing*

U. Toegang tot digitale infrastructuur en gegevens

a. Er wordt een gedocumenteerde formele en actuele procedure afgesproken voor het registreren, verlenen, wijzigen en intrekken van logische toegang tot IT- en OT-systemen. Deze procedure wordt periodiek (minimaal eens per jaar) beoordeeld en geactualiseerd.

b. De toegang van medewerkers van de leverancier is beperkt tot systemen bij ProRail, de leverancier en afgenomen diensten bij derden, die benodigd zijn voor het leveren van de dienst (need to know principe).

V. Toegang tot fysieke infrastructuur*

W. Wijzigingsbeheer

b. Substantiële wijzigingen van de leveranciersorganisatie en -processen met impact voor ProRail dienen door de leverancier tijdig kenbaar gemaakt te worden aan ProRail. Dit wordt opgenomen als onderdeel van de overeenkomst met de leverancier.